International Atomic Energy Agency cyber security conference to advise nuclear power industry

by Sam Payne

Nuclear power plant cyber security specialists from all over the world convened in Idaho Falls to collaborate on cyber security improvements at nuclear power plants. Idaho National Laboratory (INL) instrumentation and control systems specialists hosted the conference for the International Atomic Energy Agency (IAEA), the world's premier intergovernmental group dedicated to the advancement of safe nuclear technologies and nonproliferation.

The conference included presentations from a number of organizations from 12 nations. Discussions at the end of the week tackled three main problem areas by identifying administration access problems, technical weaknesses and managerial rifts regarding cyber security.

IAEA Technical Meeting attendees pose for a picture near the Snake River in Idaho Falls. Organizations from 12 different countries sent delegates to discuss cyber security issues facing nuclear power plants worldwide.

"The INL was very informative and they showed what great research is going on here," said Oszvald Gloeckler, the IAEA scientific secretary for the Technical Working Group on Nuclear Power Plant Control and Instrumentation from Hungary, and the conference organizer. "It was a great match for the IAEA, too, to come here. We got to see what kind of information was suggested by industry experts from all over the world. It was very successful in many different ways."

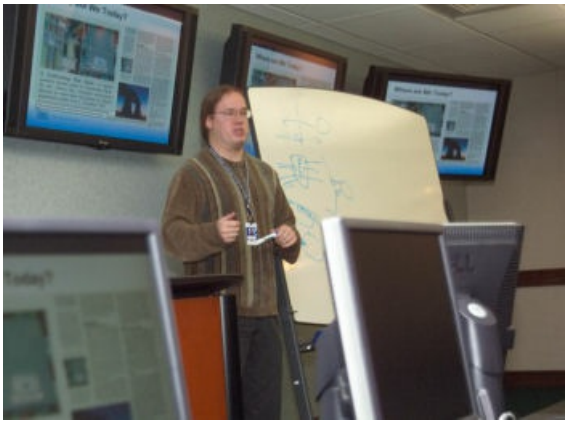
Cyber researchers Jason Larsen and Gordon Rueff demonstrate how a hacker can break into a control system network.

The age of fluid information and immediate response over the Internet dramatically increases the need for cyber security. Hackers and virus doctors run rampant in the virtual world where they can sneak their way into a company's systems from the other side of the globe. To address these threats, cyber security research and development increased to almost $310 billion in 2005.

The risk of a technology or control breach is real enough. Other industries have suffered at the hand of cyber terrorists. Citibank lost $10 billion to hackers in Russia, and the L0pht group, a type of consumer reports agency for the cyber security industry, exposed weaknesses at the Pentagon.

"The focus of the conference was on making an expert recommendation for an IAEA paper to advise nuclear power plants around the world on best practices for securing their instrumentation and control systems," said Bruce Hallbert, INL's Human Factors and Instrumentation and Control Systems Department manager, and host of the conference. "These recommendations will most likely help other industries protect and safeguard their information and infrastructure as well."

The aftermath of the Three Mile Island and Chernobyl accidents put the commercial nuclear power industry on center stage, and events in this industry continue to receive intense media attention.



"If there was a breach in security at a reactor plant, the repercussions would be very severe," said information security consultant Timo Wiander from Finish research center VTT, the largest contract-research organization in northern Europe. "If you remember Chernobyl, there have been hardly any new plants since then because of it. It took a long, long time for the public to even talk about nuclear power again. From our point of view, it's vital that industry ensures the safety and security, including cyber security, of nuclear power plants worldwide."

Clearly, the public still has concerns about the security of nuclear energy as a whole;

therefore, even the appearance of a cyber security failure at a nuclear power plant can damage public confidence in the industry. Consequently, much of the nuclear power industry's future will be determined by cyber security professionals' abilities to protect and secure the business from virtual intruders posing real threats.

Jason Larsen provides an example of how the hacker community is keeping an eye on the nuclear power industry.

"We've said for some time now that an attack on one nuclear power plant is essentially an attack on all nuclear power plants," concluded Hallbert. "It's efforts like these that will help us influence and convince others of the importance of I&C [instrumentation and control systems] at nuclear power plants all over the world."

General Contact:
Communications,

Feature Archive